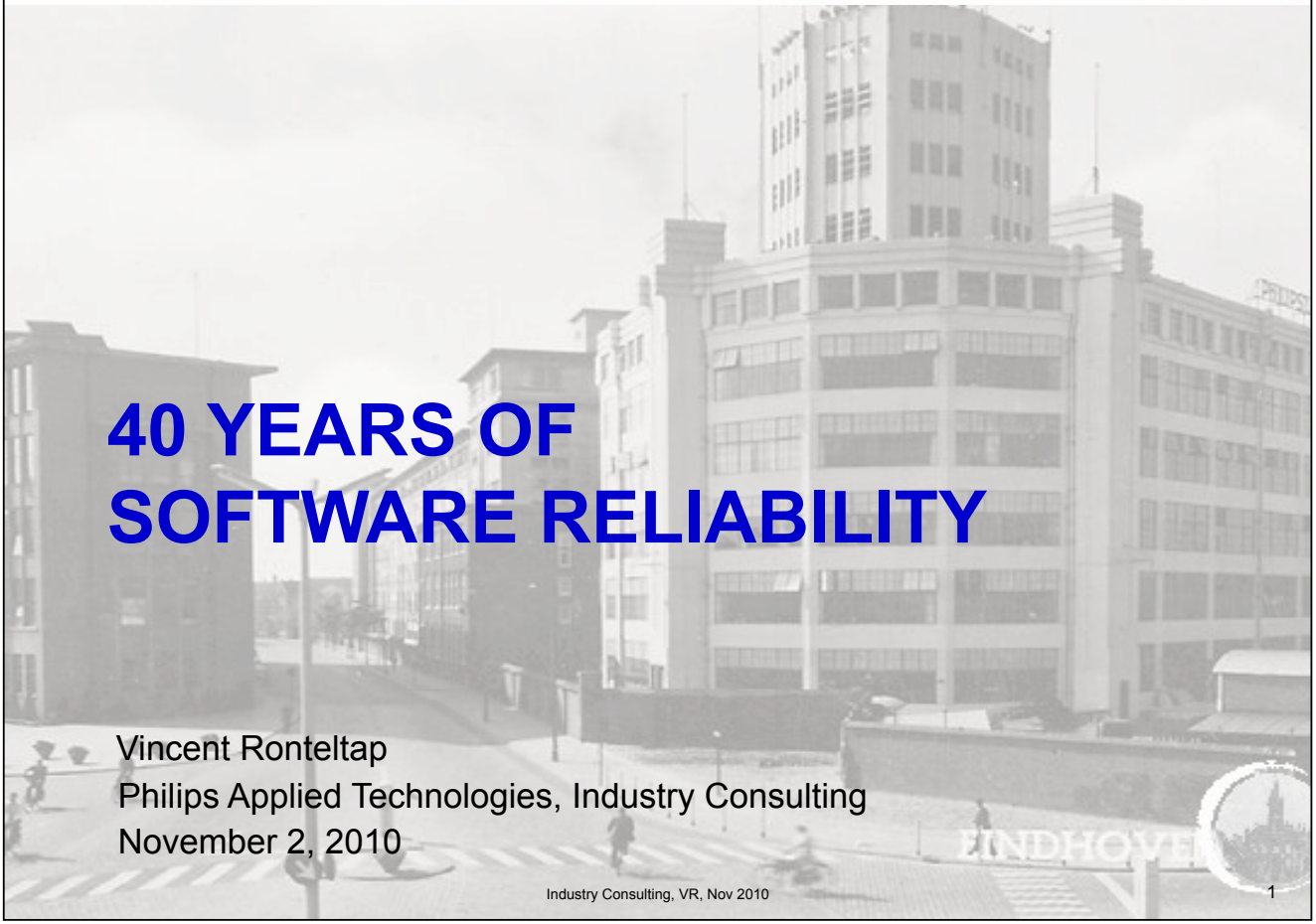
PHILIPS

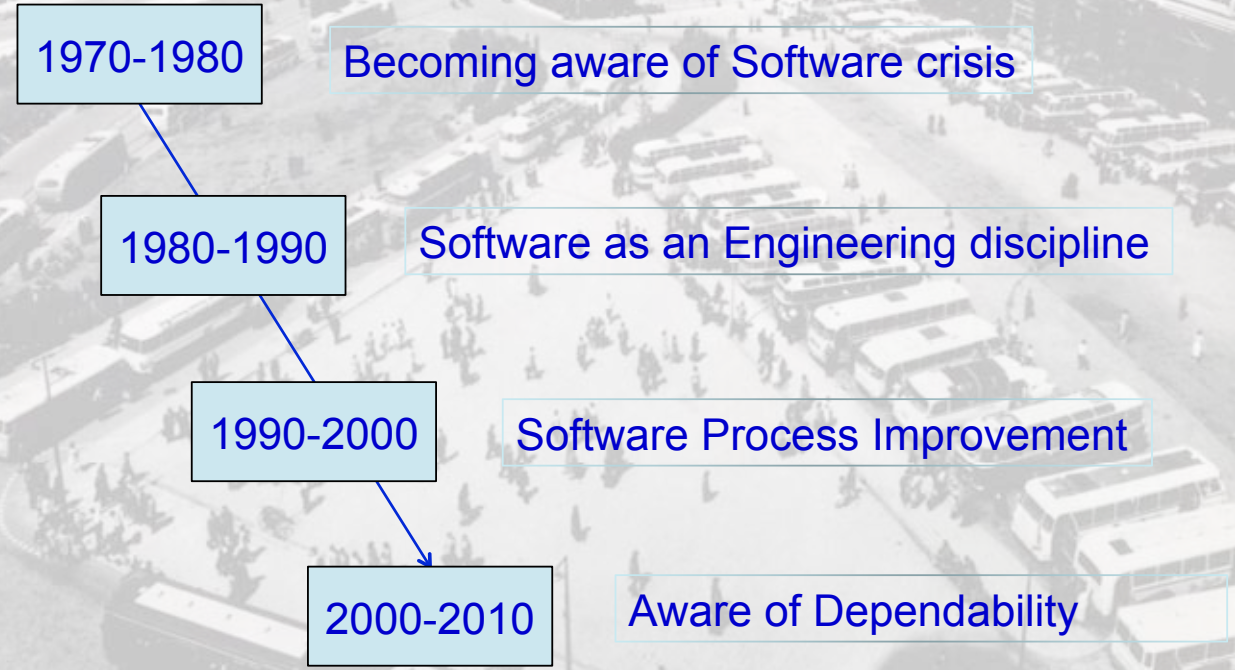


40 YEARS OF SOFTWARE RELIABILITY

Vincent Ronteltap
Philips Applied Technologies, Industry Consulting
November 2, 2010

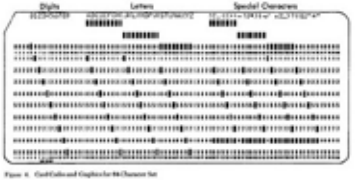
PHILIPS

4 Decades of software quality and reliability



PHILIPS

1970-1980



PHILIPS

Structured Programming

- Goto considered harmful
- The Art of Programming

"Simplicity is prerequisite for reliability."

- Stepwise Refinement
- Pascal

"Java is almost Oberon, clad in the ugly clothes of C Syntax."

- Data Abstraction

"There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies. The first method is far more difficult."

PHILIPS

Reliability is Correctness

- Growth in High-level programming languages
  - simple static data structures
  - ‘religious’ discussions on most reliable language
- How to program?
  - Formal functional specification of small programs
  - Program proofs and design
  - Hardly attention for non-functional requirements
- Hardware dominated products
  - Embedded software systems on small scale

PHILIPS

1980-1990

PHILIPS

Software Engineering

- System Analysis and Design

"Strategies for Real-time systems."

- Object Oriented Analysis, Design and Programming

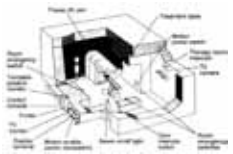
"Contracting for Software Reliability"

PHILIPS

"Complexity is the enemy of Reliability"

- All purpose languages and multitasking operating systems
  - object orientation and synchronization primitives
  - interest in software fault tolerance
- Software development seen as an Engineering discipline
- Embedded systems become an Organizational challenge
  - Painful awareness of software unsafety for the society





PHILIPS

1990-2000

PHILIPS

‘Software Process Improvement’

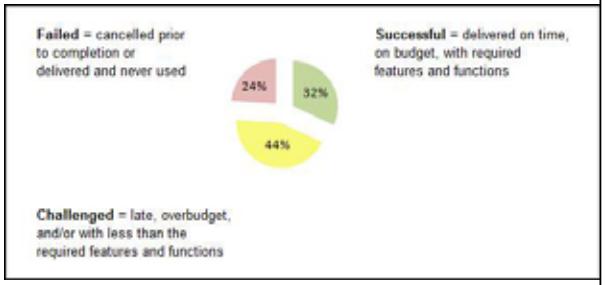
CMMI

System & Software Performance Improvement

“If you don't know where you are, a map won't help.”

PHILIPS

Process Quality to get Product Quality



- 'How to program' is understood
  - but mostly not practiced
- Development of more and more complex products is the integrated activities of multidiscipline projects
- Society expects highly reliable products
  - Reliability = Safety + Availability

PHILIPS

2000-2010

PHILIPS

‘Software Reliability’

- Test efficiency using Operational Profiles

“More Reliable Software Faster and Cheaper”

- Orthogonal Defect Classification

“ODC - a 10x for Root Cause Analysis”

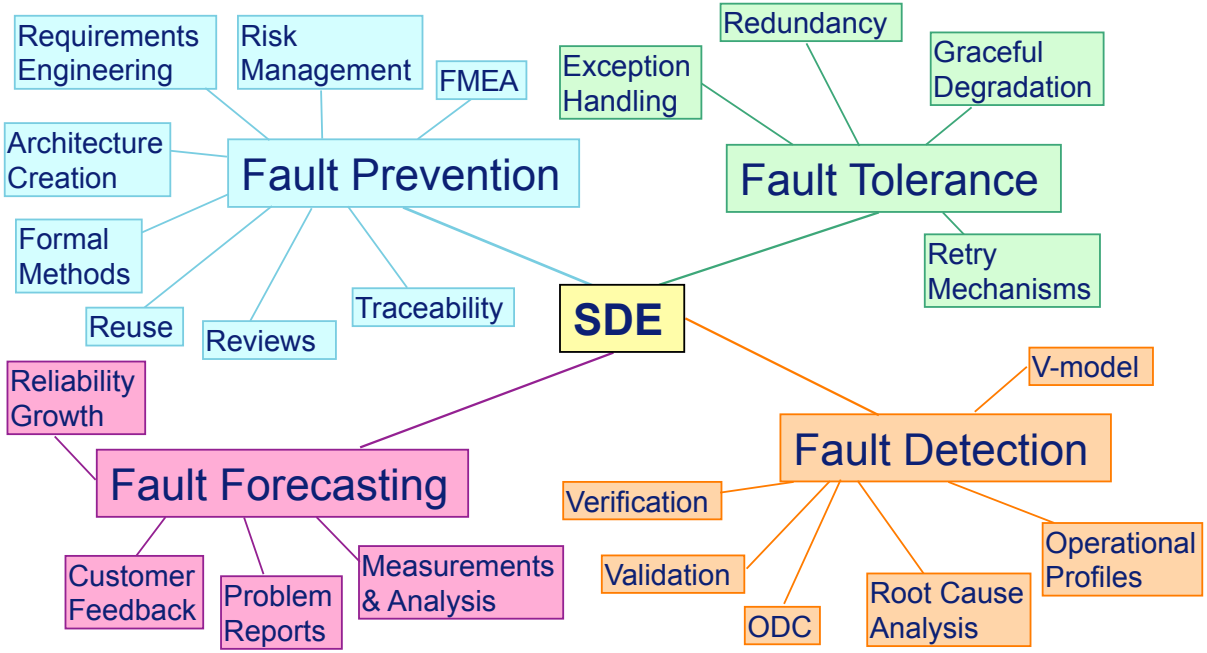
PHILIPS

Reliability becomes Dependability

- Programming seem to have become gluing components
- Growth in maturity in product development organizations
  - start of integration of quality approaches
- Society expects highly dependable products
  - Continuous operation without any interruption
  - Dependability = safety, reliability, availability, integrity, security, confidentiality, maintainability, trustworthiness, ……

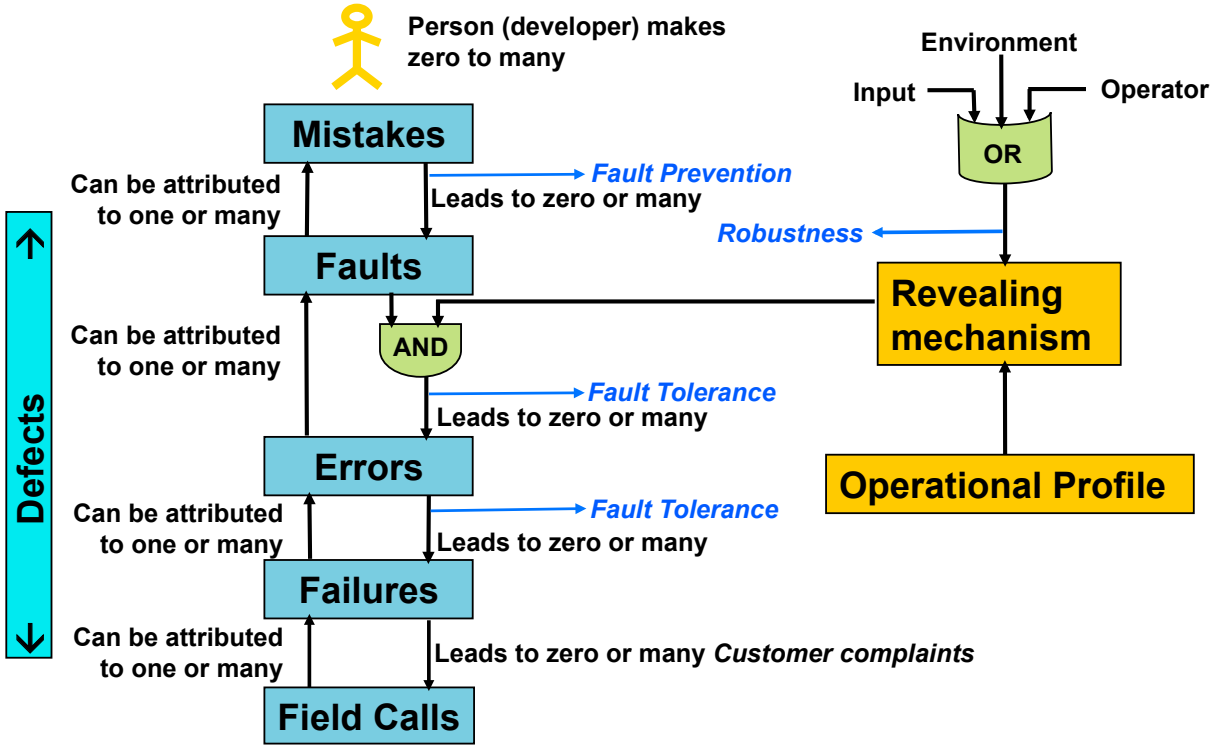
PHILIPS

Software Dependability Engineering



PHILIPS

Dependability threats



PHILIPS

What is a software Fault Tolerant system?

- A software system that continues to provide its services, even in the presence of errors or faults, is fault tolerant
  - *Possibly in degraded mode*
- A fault ***in***tolerant software system avoids making errors and faults (zero defects)

PHILIPS

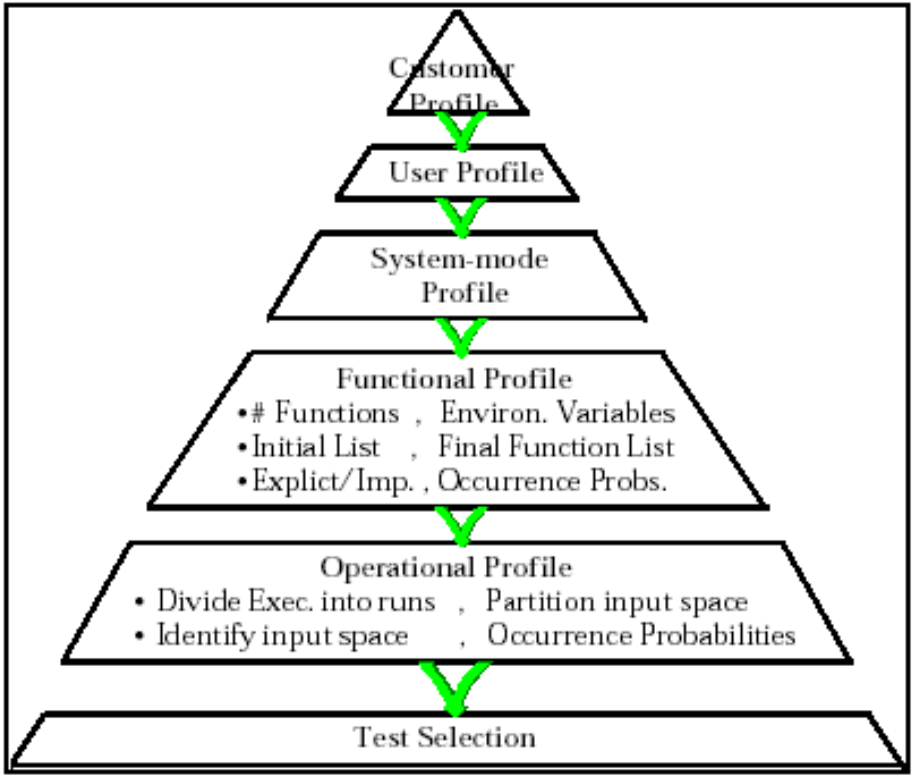
Operational Profile

A quantitative characterization of how a system will be used in the field by making a partition of the input space

A set of operations and their probabilities of occurrence

PHILIPS

Developing Operational Profiles



PHILIPS

SR Testing, User-centered testing

- Software is tested as it is going to be used
- Operational Profiles indicate mostly used functions
  - few faults may cause majority of failures
- High-rate failures are found first
- Focuses on external behavior, not on internals
- Reliability is measured from the user's point of view
- Is a common-sense addition to Risk Based Testing

PHILIPS

What is Orthogonal Defect Classification?

An accident requires multiple failures

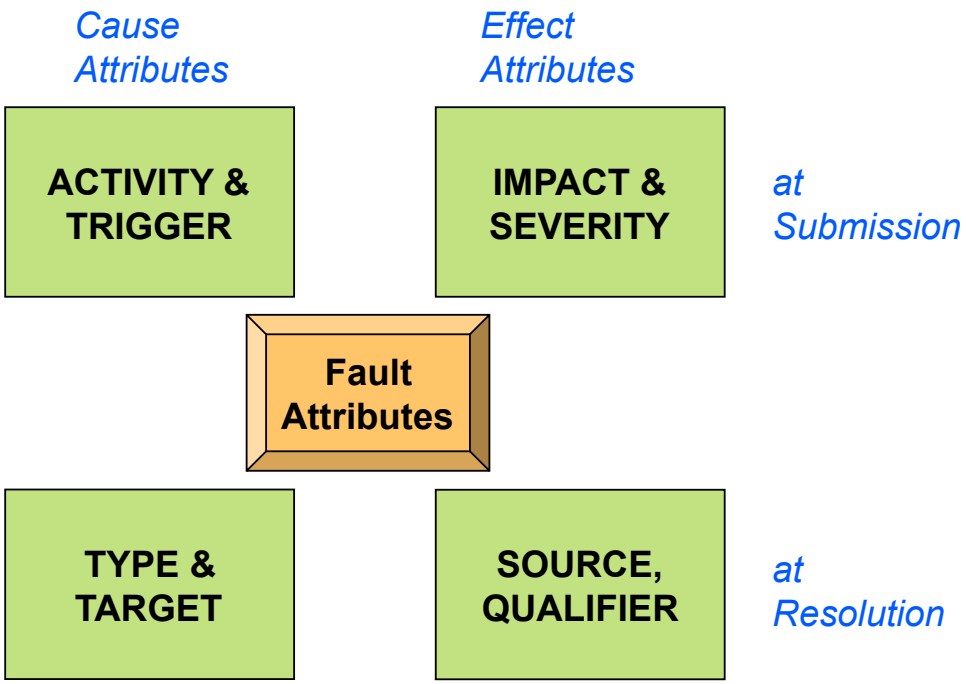
- single point failures are not enough
- each of these failures is necessary to cause it

ODC is a scheme that helps capture defect information

In ODC, defects are categorized into classes, that will ultimately point to the software processes that needs attention

PHILIPS

ODC: Fault Attributes



PHILIPS

software versus hardware 1/2

Software defects are mainly *development defects*

- occur mostly without warning and can hardly be anticipated, unlike hardware

Redundancy

- Identical software components do not increase Sw Reliability

Wear-out Software does not deteriorate

- no energy related wear-out
- no physical (thermal, electro-magnetic, pressure) or chemical influences

Software is hardly built yet with reliable standard components

PHILIPS

software versus hardware 2/2

Basically,

software is deterministic;

output = F (input)

so there is no inherent stochastic variability

Failure rates for software *components* are hardly known

Reliability prediction

Software failure rate is not predictable from analyses of design or program text

Hardware reliability is more common practice

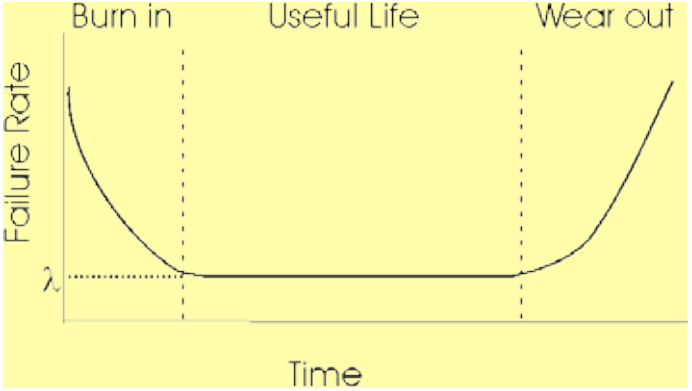
– and much more mature than software reliability

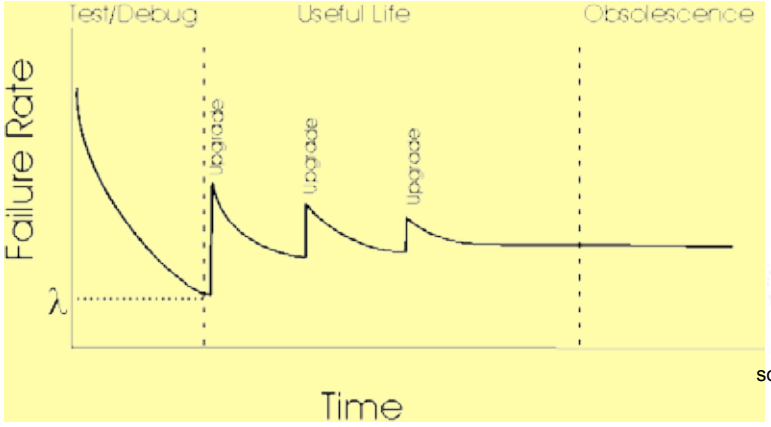
MTBF, MTBC, MTTF for software need separate definition

– Operational time or test execution time may be used, instead of clock time

PHILIPS

‘Bathtub’ curves hardware and software





software aging

PHILIPS

Note on variability of software

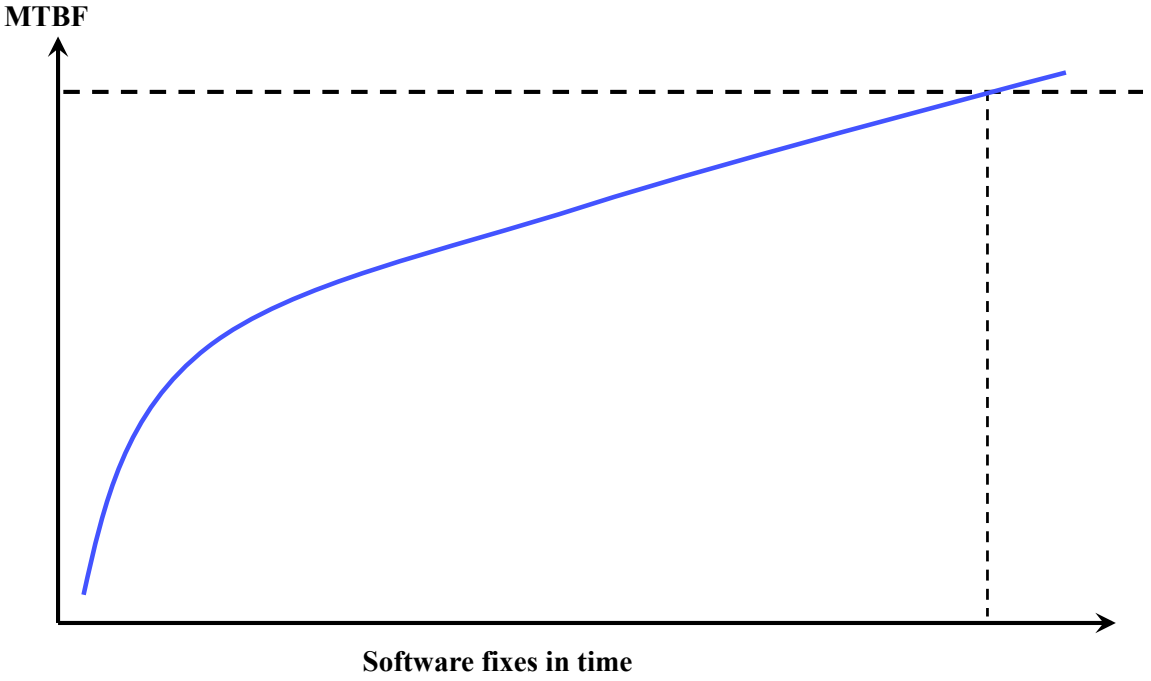
Running Complex software systems with many possible causes for failures do show stochastic (probabilistic) failure behavior,

due to

- variations in inputs
- variations in the execution environment
- occurring hardware anomalies

PHILIPS

Software Reliability Growth



PHILIPS

… and from now?

- Integration of dependability approaches, based on CMMI-Dev as a guiding reference model
- Merge of hardware and software in system dependability
- Organizations will wish to know
  - how to master the extreme complexity?
  - how dependable are the products at final release?
  - how much service, maintenance do we need?

PHILIPS

Whatever is worth doing, is worth doing well

- Earl of Chesterfield

PHILIPS


PHILIPS